European Union General Data Protection Regulation and Data Transfer Addendum

This Data Processing Addendum ("**Addendum**") is part of and modifies the following iOFFICE service agreements, including, without limitation: the Online Services Agreement, the Master Services Agreement, and the Master Subscription Agreement (hereinafter, whether expressly named or not, collectively and severally referred to, "**Agreement**" or "**the Agreement**"). This Addendum is by and between iOFFICE of 1210 W. Clay Street, Houston, Texas ("**Processor**" and/or "**Data Importer**"), on the one hand, and the Data Controller ("**Controller**" and/or "**Data Exporter**") on the other, the latter either executing this Addendum by written execution or through website forms, or having been deemed a party to the Addendum by having been made aware of its contents and electing not to seasonably object. This Addendum is made and entered into as of the date of the Agreement or May 25th, 2018, whichever is later (the "**Effective Date**"). Controller and Processor are sometimes referred to herein individually as a "Party" and collectively as the "Parties."

For the purposes of this Addendum and unless otherwise stated, the capitalized terms herein shall have the same meaning as the definitions used in GDPR or in the Standard Contractual Clauses for the Transfer of Personal Data to Data Processors established in Third Countries, which are contained in the annex to the "European Commission decision 2010/87/EC of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries" ("Standard Contractual Clauses", or "Clauses" attached hereto as Annex 1)**,** or the meaning assigned to such terms in the Agreement.

This addendum applies only where data is collected from offices or data subjects residing in the European Union ("EU") or data regarding data subjects is processed in the EU.

RECITALS

WHEREAS, the Parties have entered into the Services Agreement for the purposes of providing services as outlined in the Agreement, including but not limited to facilities and office management;

WHEREAS, pursuant to Processor's provision of services pursuant to the Agreement, Processor may receive custody of or store, process, or gain access to data of Controller's customers or its employees as further described in Appendix 1 hereto; and

WHEREAS, the Parties wish to ensure that adequate safeguards are in place with respect to the protection of the privacy of Data Subjects pursuant to the European Union General Data Protection Regulation (as amended or replaced from time to time) ("**GDPR**") and therefore wish to amend the Agreement under the terms and conditions set forth herein; and

WHEREAS, European data protection laws require data exporters in EU/EEA countries to provide adequate protection for transfers of personal data to non-EU/EEA countries, and such protection can be adduced by requiring the data importers to enter into the Standard Contractual Clauses for the Transfer of Personal Data to Third Countries pursuant to Commission Decision 2004/915/EC of 27 December 2004 (as amended or replaced from time to time).

NOW, THEREFORE, for and in consideration of the mutual promises and covenants herein contained, and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties hereto hereby agree as follows:

AMENDMENTS TO AGREEMENT

1. AMENDMENTS TO AGREEMENT

1.1 Amendment. The Parties hereby agree that the Agreement shall be amended by adding to the Agreement this Addendum.

1.2 Effect of Addendum. All provisions of the Services Agreement not specifically amended hereby shall remain in full force and effect. In the event of any irreconcilable conflict between the provisions of this Addendum and any provisions of the Services Agreement, the provisions of this Addendum shall prevail. Should a provision of this Addendum be or become invalid, the validity of the other provisions of this Addendum shall remain unaffected hereby, and each term and provision hereof shall be valid and enforced to the fullest extent of the law.

1.3 Further Amendments. The provisions of the Agreement, including the provisions of this clause, may not be amended, modified or supplemented, and waivers or consents to departures from the provisions of the Agreement may not be given, without the prior written consent thereto by each Party's authorized representative. No waiver by either Party of any default, misrepresentation, or breach of warranty or covenant hereunder, whether intentional or not, will be deemed to extend to any prior or subsequent default, misrepresentation, or breach of warranty or covenant hereunder or affect in any way any rights arising by virtue of any prior or subsequent such occurrence.

2. DATA PROCESSING

2.1 Controller Instructions. Processor shall process Personal Data of Controller only on behalf of and for the benefit of Controller and pursuant to documented instructions from the Controller. The Parties expressly agree and stipulate that the Agreement, including applicable service level agreements or equivalent documents, shall constitute the Controller's written instructions to Processor. Any additional processing instructions must be mutually agreed to in writing by the Parties. Processor shall immediately inform Controller if, in Processor's opinion, an instruction infringes Applicable Law.

2.2 Authority to Transfer to Processor. Controller represents and warrants that Controller has the authority and right, including consent where required, to lawfully transfer to Processor all Personal Data and any other data or information related to Controller's access or use of the Services.

2.3 Compliance with Applicable Law. Controller represents and warrants that it shall comply with (i) all applicable international, federal, state, provincial and local laws, rules, regulations, directives and governmental requirements currently in effect and as they become effective relating in any way to the privacy, confidentiality, and/or security of Personal Data, including, but not limited to, GDPR; (ii) all applicable industry standards concerning privacy, data protection, confidentiality or information security including, without limitation the Payment Card Industry Data Security Standard ("PCI DSS"); and (iii) applicable provisions of Processor's written requirements currently in effect and as they become effective relating in any way to the privacy, confidentiality, and/or security of Personal Data or applicable privacy policies, statements or notices that are provided to Controller by Processor in writing (collectively, "**Applicable Law**").

3. SUB-PROCESSORS

3.1 Engagement of Sub-processors. Controller expressly acknowledges and agrees that (a) Processor may retain any entity which is controlled by, controls or is in common control with Processor ("**Affiliates**") in connection with the provision of the Services; and (b) Processor and Processor's Affiliates respectively may engage other third-party processors in connection with the provision of the Services (collectively, "**Sub-processors**").

3.2 Obligations of Sub-processors. Any Sub-processors will be permitted to process Personal Data only as necessary to deliver the services for which Processor has retained them, and such Sub-processors are prohibited from processing Personal Data for any other purpose. Such Sub-processors will provide services pursuant to a written agreement containing the same data protection obligations as set forth herein. Processor shall be liable to Controller for the acts and omissions of its Sub-processors to the same extent Controller would be liable if performing the services of each Sub-processor directly under the terms of this Addendum, except as otherwise set forth in the Agreement.

3.3 List of Sub-processors. Upon Controller's request, Processor shall make available to Controller a current list of Sub-processors for the respective Services with the identities of those Sub-processors ("**Sub-processor List**").

4. CONFIDENTIALITY

4.1 Confidentiality. Processor will treat Personal Data of Controller as confidential. Processor will ensure that its personnel engaged in the processing of Personal Data of Controller are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and are subject to obligations of confidentiality and that such obligations survive the termination of that persons' engagement with Processor.

5. SECURITY

5.1 Security Measures. Processor shall implement appropriate technical and organizational measures to protect the security, confidentiality, integrity, and availability of Personal Data of Controller, as set forth in further detail in Appendix 2.

5.2 Data Breach Notification. Processor shall promptly notify Controller of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data of Controller ("**Data Breach**") after having become aware of such Data Breach. Notification(s) of Data Breaches, if any, will be delivered to Controller's designated contact by means as agreed to by the Parties. It is Controller's sole responsibility to ensure it maintains accurate contact information for purposes of such notification.

6. ASSISTANCE TO CONTROLLER

6.1 Data Subject Rights. Where possible, and taking into account the nature of the processing, Processor will provide commercially reasonable assistance to Controller for the fulfillment of Controller's obligation to respond to requests for exercising data subjects' rights as set forth in GDPR, Articles 12-23.

6.2 Security and Data Protection Impact Assessments. Processor will provide commercially reasonable assistance to Controller for the fulfillment of Controller's obligations pursuant to GDPR, Article 32 (security of processing) and Article 36 (prior consultation), as appropriate and feasible with respect to the nature of processing and information available to Processor.

6.3 Audits and Inspections. Processor shall make available to Controller information necessary to demonstrate compliance with the obligations set forth in GDPR, Article 28. Processor shall allow for and contribute to audits, including inspections, conducted by Controller or another auditor mandated by Controller. Controller shall reimburse Processor for any time expended for any such on-site audit at Processor's then-current professional services rates, which shall be made available to Controller upon request. Before the commencement of any such on-site audit, Processor and Controller shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Controller shall be responsible. The Parties shall work in good faith to schedule the audit at a time that is mutually beneficial, and so as to avoid

unreasonable disruption Processor's business operations. All reimbursement rates shall be reasonable, taking into account the resources expended by Processor. Unless otherwise agreed to in writing by the Parties, Controller shall bear the costs associated with the performance of audits of Processor conducted pursuant to this provision. Controller shall promptly notify Processor with information regarding any non-compliance discovered during the course of an audit relevant to the Services or this Agreement.

7. DATA TRANSFERS

7.1 Transfer to United States. Controller expressly acknowledges that some or all of the Services may be provided and/or hosted from within the United States. Controller expressly consents to the transfer of Controller's Personal Data to the United States for purposes of Processor providing the Services and performing its obligations under the Agreement. Such transfers will be conducted pursuant to this Agreement, including Annex 1 (Standard Contractual Clauses).

8. PERSONAL DATA DELETION

8.1 Deletion or Return of Controller Personal Data. Unless otherwise required by law, Processor will delete or return Personal Data of Controller within a reasonable time period upon: (i) expiration or termination of the Agreement, or (ii) Controller's lawful, written request.

8.2 Certification. The Parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of Annex 1 (Standard Contractual Clauses) shall be provided by Processor to Controller upon Controller's request and as permitted by law.

9. INDEMNIFICATION

9.1 Indemnification. Controller agrees to indemnify and hold harmless Processor and its Affiliates and their respective current, future and former officers, employees, directors, agents, successors and assigns (collectively, "Processor Indemnitees") from, and at Processor's option defend against, any and all Losses (as defined below) that Processor Indemnitees may incur, to the extent that such Losses arise from, or may be in any way attributable to: (i) any violation of this Addendum; and (ii) the negligence, gross negligence, bad faith, fraudulent acts or omissions, or intentional or willful misconduct of Controller or its personnel in connection with obligations set forth in this Addendum. For purposes of this Addendum, "Losses" means all judgments, settlements, awards, damages, losses, charges, liabilities, penalties, interest claims (including taxes and all related interest and penalties incurred directly with respect thereto), and all related reasonable costs, expenses and other charges (including all reasonable attorneys' fees and reasonable internal and external costs of investigations, litigation, hearings, proceedings, document and data productions and discovery, settlement, judgment, award, interest and penalties).

10. MISCELLANEOUS

10.1 Counterparts. This Addendum may be executed in counterparts, each of which shall be deemed an original and all of which together shall constitute one and the same document.

10.2 Duration and Termination. All notices for termination must be in writing and comply with the procedures for termination set forth in the Agreement. Unless otherwise agreed to in writing by the Parties, this Addendum shall remain in effect until the expiration of the Agreement.

10.3 Survival of Terms. The rights and obligations of either Party that by their nature would continue beyond the termination or expiration of this Addendum, including but not limited to, confidentiality obligations, shall survive termination or expiration of this Addendum.

10.4 Entire Agreement. This Addendum (which shall be incorporated into the Agreement and form an integral part thereof) constitutes the entire agreement and understanding between the Parties and supersedes all prior and contemporaneous verbal and written negotiations, agreements and understandings, if any, on the specific subject matter of this Addendum, and this Addendum cannot be modified except pursuant to written agreement, signed by an authorized representative of each Party.

10.5 Severability. In case any provision in this Addendum shall be invalid, illegal or unenforceable in any jurisdiction that provision shall, as to such jurisdiction, be ineffective to the extent of such invalidity, illegality or unenforceability without affecting the validity, legality and enforceability of the remaining provisions; and the invalidity of a particular provision in a particular jurisdiction shall not invalidate such provision in any other jurisdiction.

Annex 1

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, the Data Importer and Data Exporter, each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[1]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

[1] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):

Data Exporter uses the Data Importer's services for the full scope of activities outlined in the Agreement, which are incorporated herein by reference, as if fully set forth at length below. Without limitation, these services include automated functions to support office and facilities management.

Data importer
The data importer is (please specify briefly activities relevant to the transfer):

Data Importer processes user information for the data exporter to provide office and facilities management services, which information can include first, middle, and last name, aliases, employee ID or username, job title, mobile, work, and personal phone numbers, email addresses, mail stop, building, floor, and room location for employees, as well as other, related information, including other forms of personal data, germane to the work environment and office and facilities management.

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):

Data subjects in scope include application users, employees, owners, directors, facility visitors, customers, and vendors.

Categories of data
The personal data transferred concern the following categories of data (please specify):

Data Importer processes user information for the data exporter to provide office and facilities management services, which information can include first, middle, and last name, aliases, employee ID or username, job title, mobile, work, and personal phone numbers, email addresses, mail stop, building, floor, and room location for employees, as well as other, related information, including other forms of personal data, germane to the work environment and office and facilities management.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):

None.

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):

If AUP is utilized, a directory watcher will consume the file upon receiving. On consumption the file will be parsed into a temp table and compared to our current user set. Data importer will calculate the Delta data and update accordingly. The AUP file is then archived in a secure location where it is kept for 60 days or until space is needed, upon which it time the data is purged. Data is stored in the application is retained for reporting purposes until the end of contract.

Other processing includes, storage, the use of databases, analysis, queries, and the use of automated code to provide the services detailed in the Agreement or which are necessary or helpful to provide the services described in the Agreement.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(c) and 5(c) (or document/legislation attached):

The Data Importer also has mechanisms or processes in place to provide for:

- the pseudonymisation or encryption of data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The following specific measures are also in place, based on context:

1. Physical access control

   Measures to prevent unauthorized persons from gaining access to data processing systems for processing or using data:

   a) Definition of persons who are granted physical access;

   b) Implementation of policy for external individuals;

   c) Alarm device or security service outside service times;

   d) Implementation of measures for on-premise security (e.g. intruder alert/notification).

2. Logical access control

   Measures to prevent that unauthorized persons use data processing equipment and – procedures:

   a) Definition of persons who may access data processing equipment;

   b) Implementation of policy for external individuals;

   c) Password protection of personal computers.

3. Data access control

   Measures that ensure that persons entitled to use a data Processing system gain access only to such data as they are entitled to accessing in accordance with their access rights:

   a) Allocation of access rights using the principle of least privilege and specific to required functions;

   b) Implementation of partial access rights for respective data and functions;

c) Requirement of identification vis-à-vis the data processing system (e.g. via ID and authentication;

d) Implementation of policy on access- and user-roles;

e) Evaluation of protocols in case of damaging incidents.

4. Data Transfer control

Measures to ensure that personal data cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of personal data by means of data transmission facilities can be established and verified.

a) Encryption in transit using TLS;
b) Encryption of data at rest on SFTP servers.

5. Entry control

Measures to ensure that it is possible to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom:

a) Logging of data entry.

6. Control of instructions

Measures to ensure that personal data processed on behalf of others are processed strictly in compliance with data exporter's instructions:

a) Documentation of distinction of competences and obligations between data exporter and data importer;

b) Formal assignment process;

c) Control of work results.

7. Availability control

Measures to ensure that personal data is protected against accidental destruction or loss:

a) Realization of a regular backup schedule;

b) Control of condition and respective labelling of data carriers for data backup purposes;

c) Safe storage of data backups in fire- and water-protected security cabinets;

d) Implementation and regular control of emergency power systems and overvoltage protection systems;

e) Implementation of an emergency plan;

f) Protocol on the initiation of crisis- and/or emergency management.

8. Control of data separation

Measures to ensure that data collected for different purposes can be processed separately:

a) Logical separation of data of each of data importer's clients.